

FIG. 3

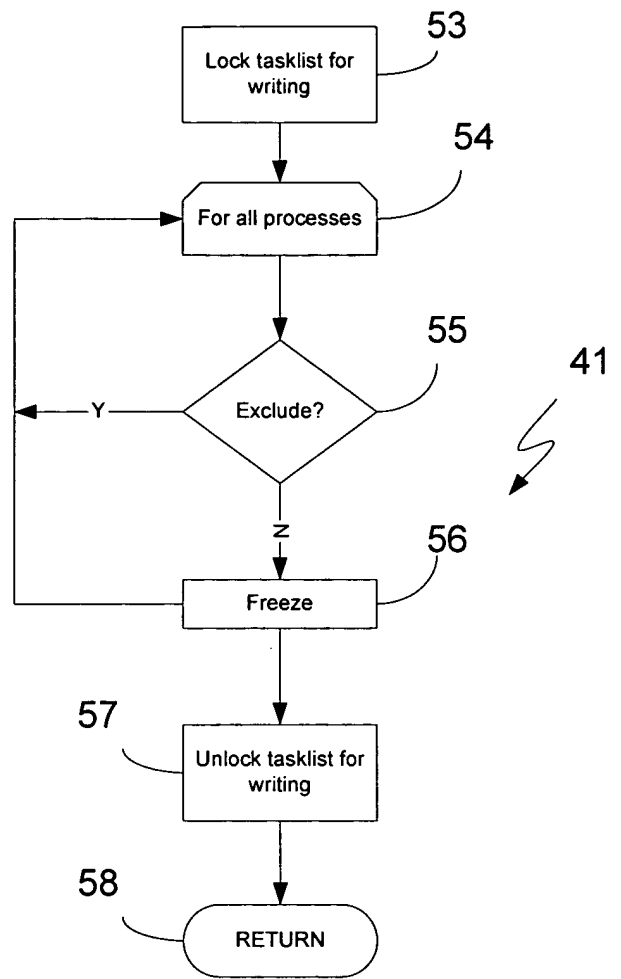


FIG. 5

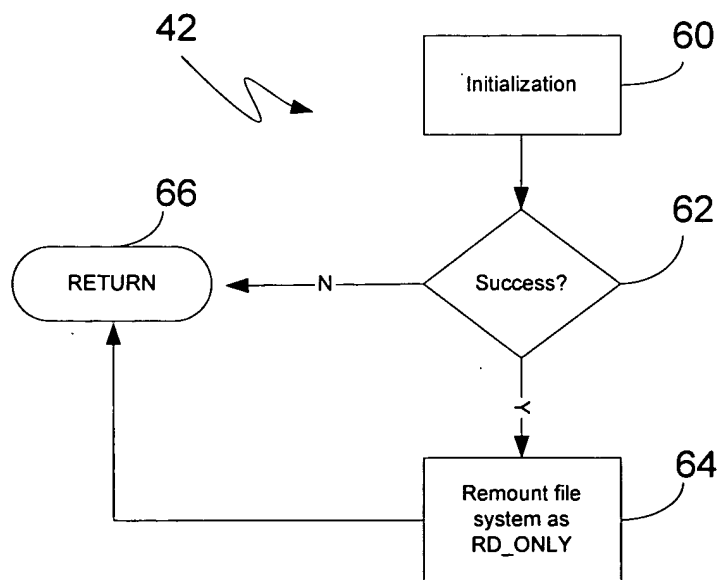


FIG. 6

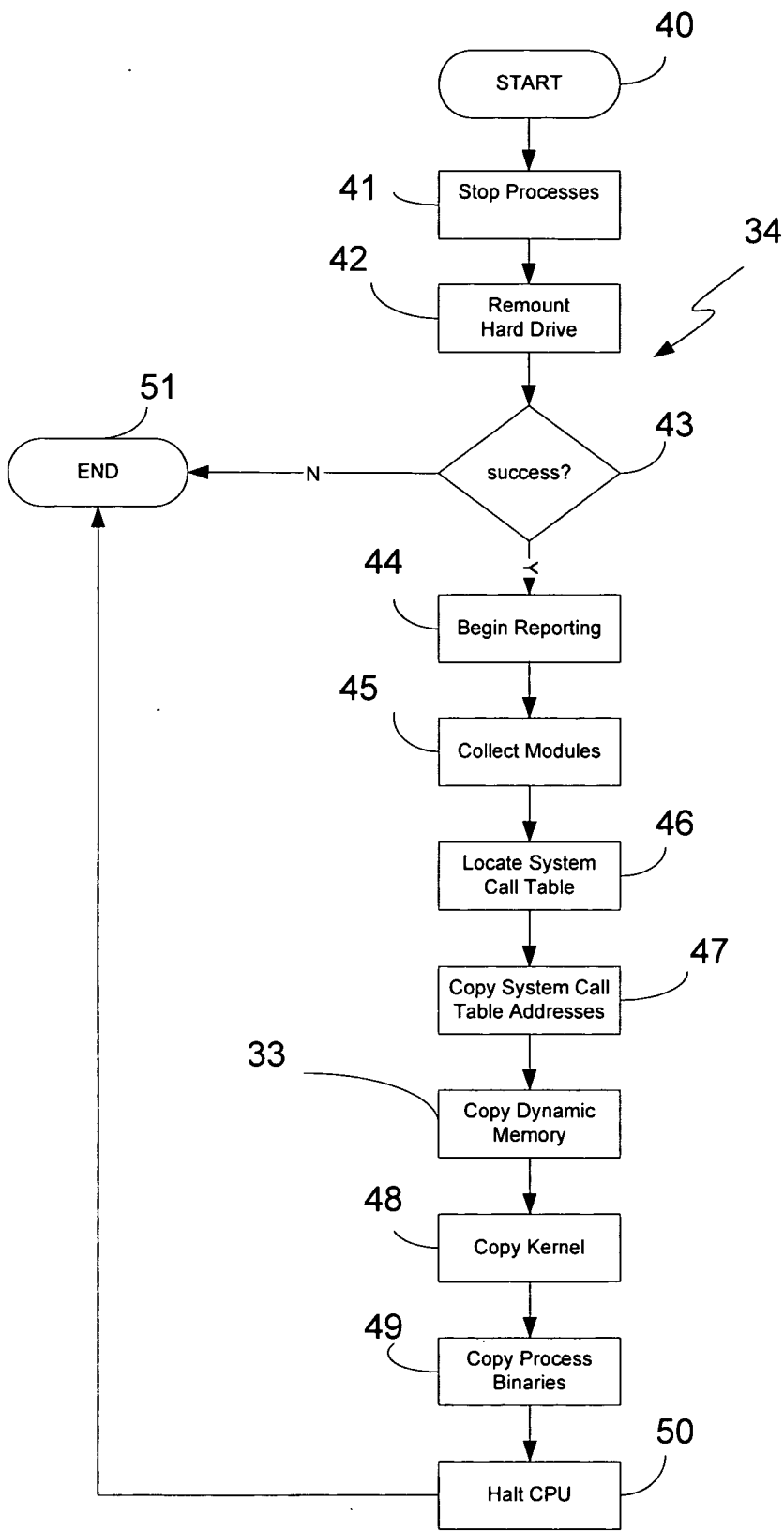


FIG. 4(a)

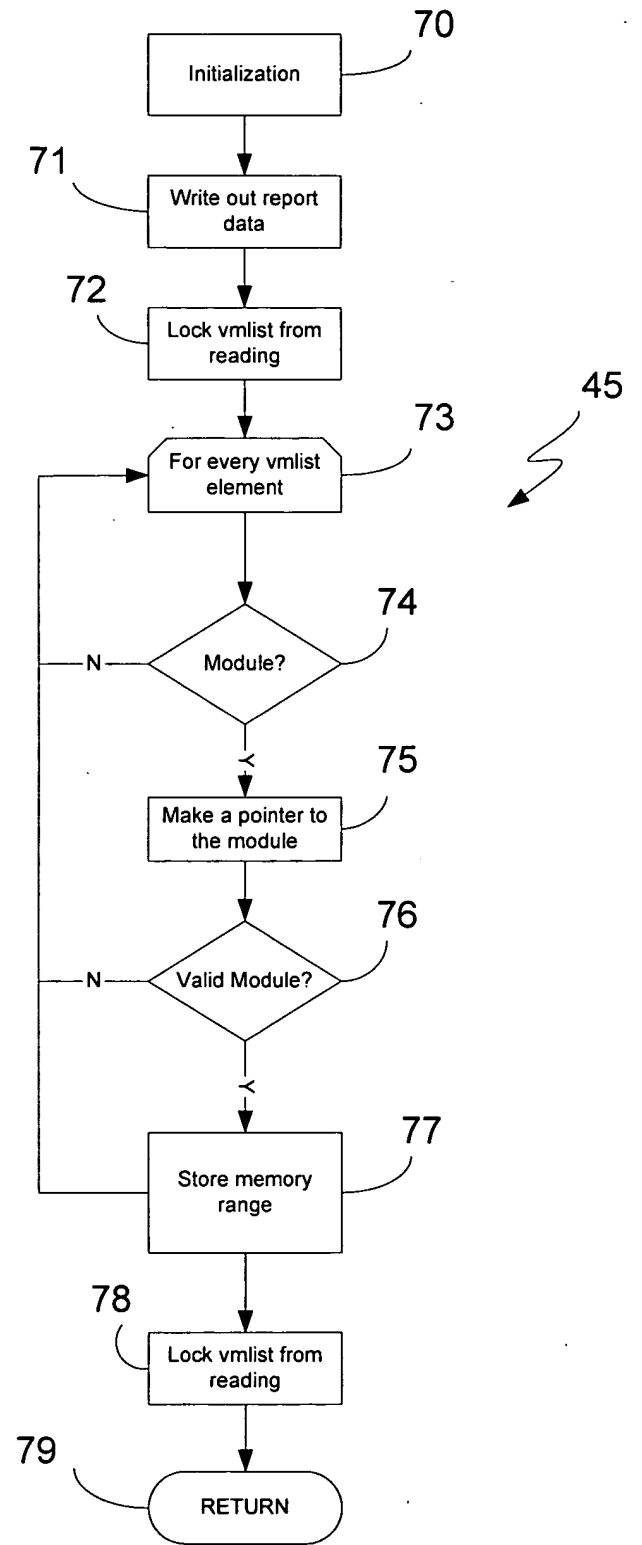


FIG. 7(a)

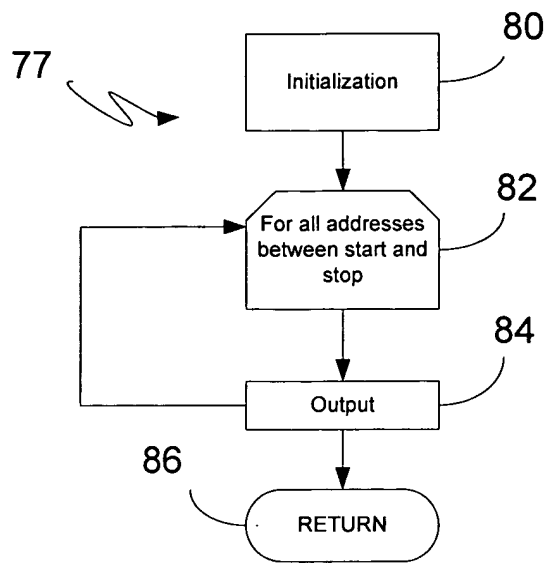


FIG. 8

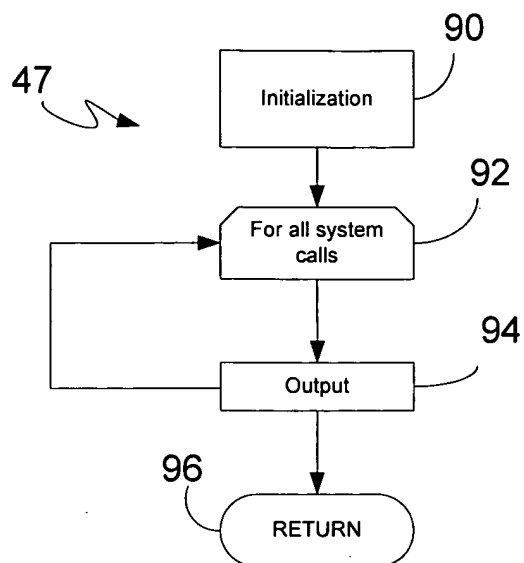


FIG. 9(a)

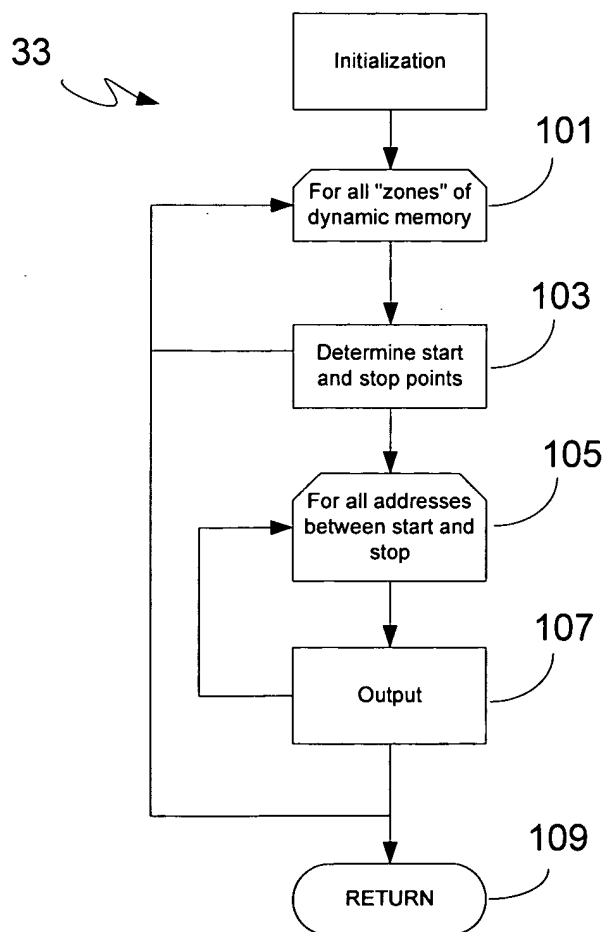


FIG. 10(a)

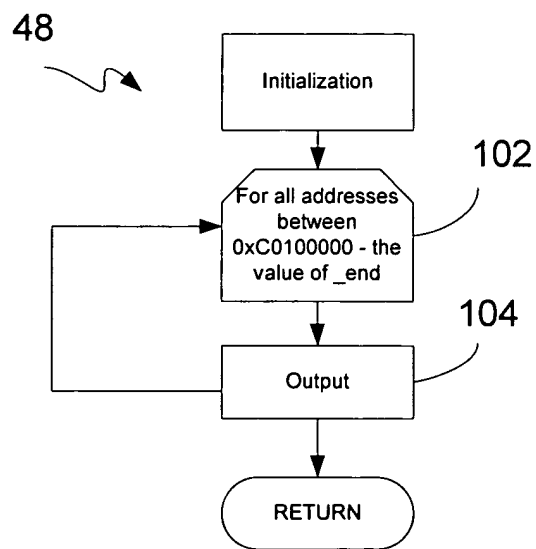


FIG. 10(c)

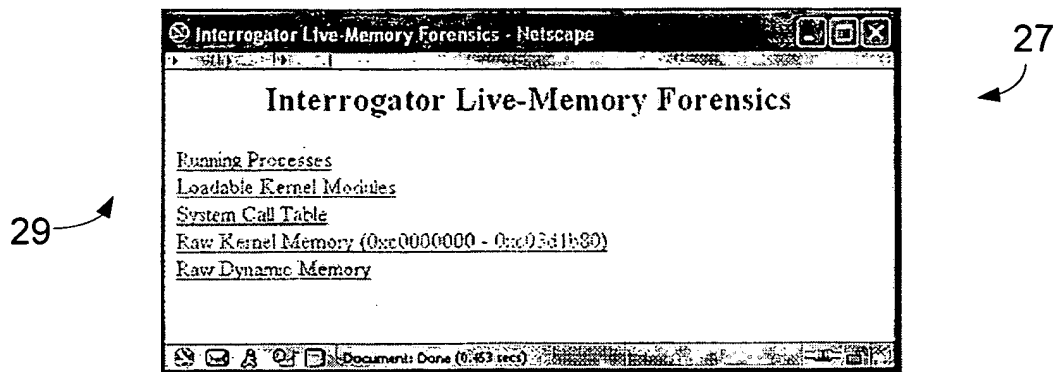


FIG. 4(b)

Loadable Kernel Modules - Netscape

module	size	refcount	address
ide-cd	33608	0	0xd08e6000 - 0xd08ee348
vmxhfs	37228	4	0xd08f0000 - 0xd08f916c
ip_tables	14936	2	0xd08fb000 - 0xd08fea58
ip_tables_filter	2412	1	0xd0900000 - 0xd090096c
nls_iso8859-1	3516	1	0xd0902000 - 0xd0902dbc
pcnet32	17856	1	0xd0906000 - 0xd090a5c0
ip_tables_REJECT	3736	6	0xd090e000 - 0xd090ee98
autofs	13348	0	0xd0910000 - 0xd0913424
soundcore	6532	0	0xd0970000 - 0xd0971984
sr_mod	18136	0	0xd0995000 - 0xd09996d8
usb-storage	62000	1	0xd09ce000 - 0xd09dd230
fat	38712	0	0xd09df000 - 0xd09e8738
vfat	13084	1	0xd09ea000 - 0xd09ed31c
nls_cp437	5116	1	0xd09ef000 - 0xd09f03fc
adcore	7968	0	0xd09f2000 - 0xd09f3f20

Document: Done (0:25 sec)

FIG. 7(b)

83

81

### System Call Table

System Call	Address	NAME
Syscall[1]	0xc011e1d0	exit
Syscall[2]	0xd09f2650	fork
Syscall[3]	0xc013fb70	read
Syscall[4]	0xd09f27e3	write
Syscall[5]	0xd09f3184	open
Syscall[6]	0xd09f2898	close
Syscall[7]	0xc011e5b0	waitpid
Syscall[8]	0xc013f180	creat
Syscall[9]	0xc014cb10	link

Document: Done (0.25 sec)

FIG. 9(b)

85

### Kernel Memory

Zone	Begin	End
DMA	0xc1000030	0xc1038030
Normal	0xc1070030	0xc13b8030
HighMem	0x0	0x0
Dynamic	0xd0800000	0xd0900000

Document: Done (0.063 sec)

FIG. 10(b)

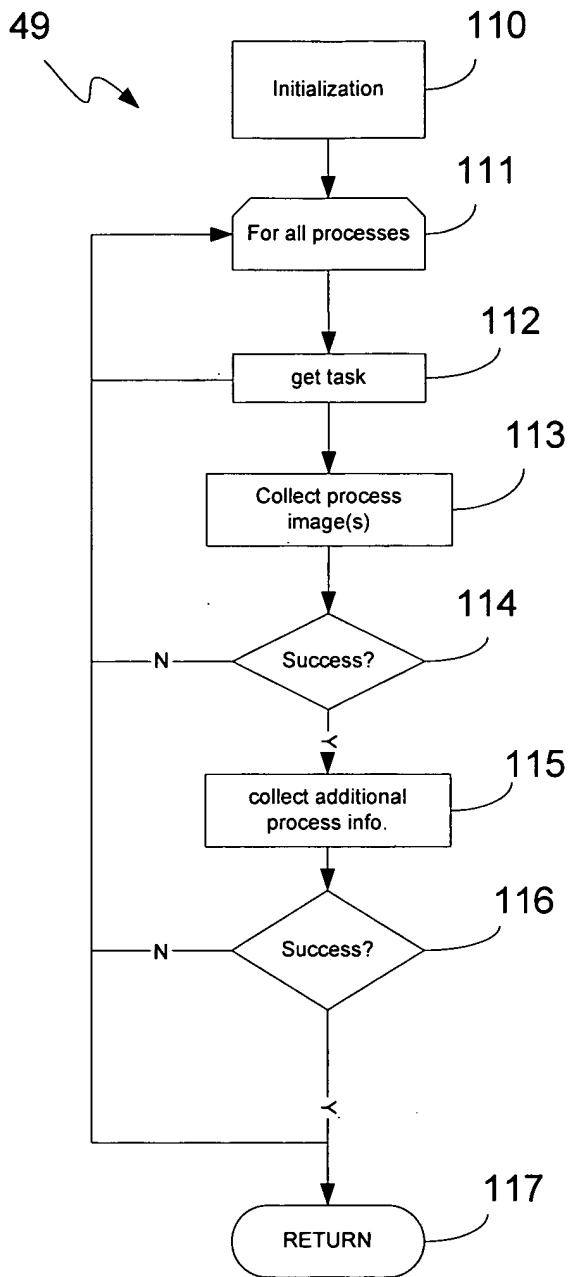


FIG. 11(a)

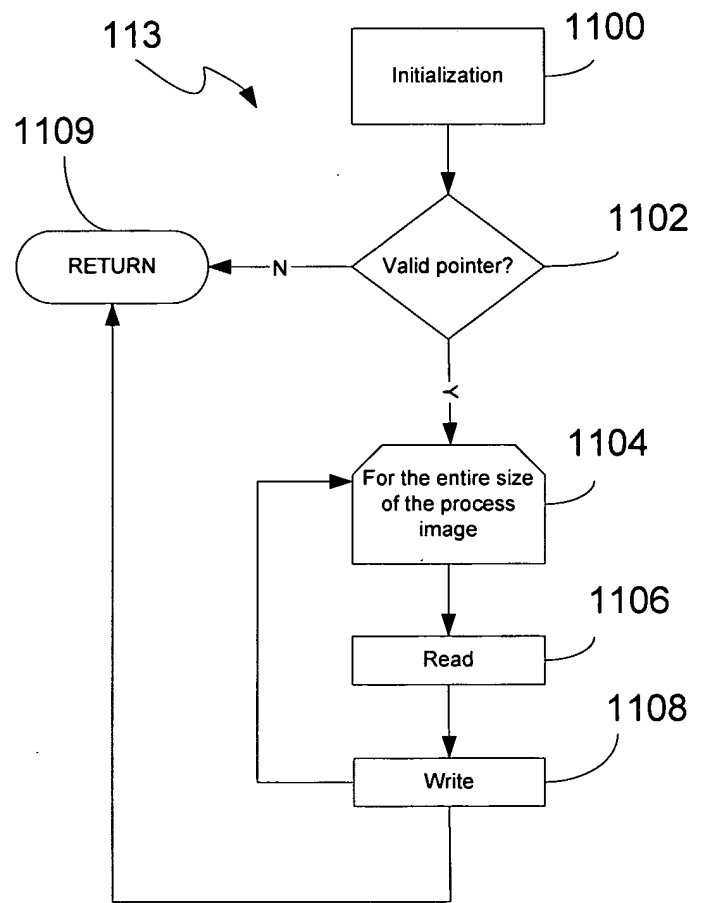


FIG. 11(b)

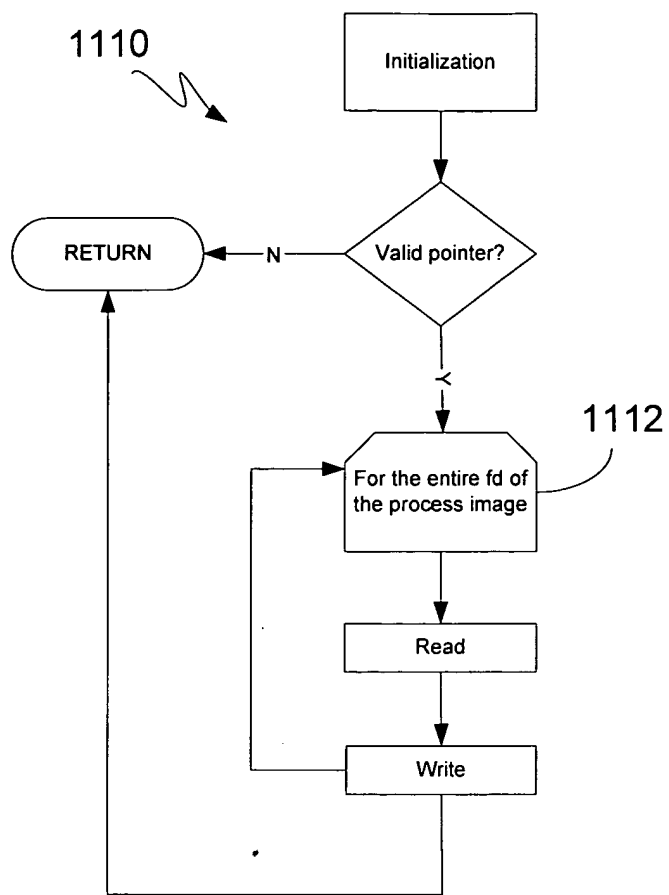


FIG. 11(c)

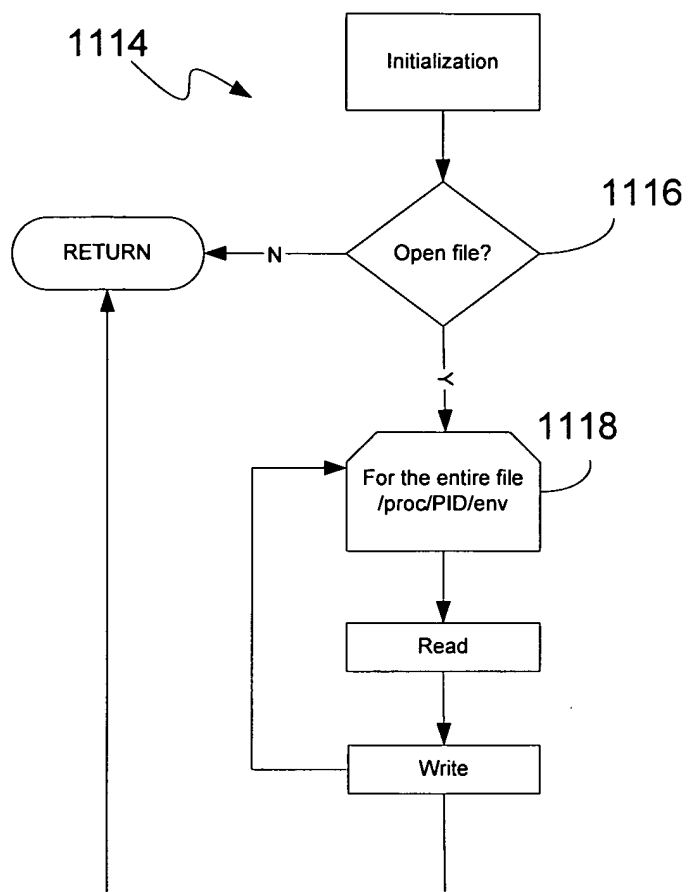


FIG. 11(d)

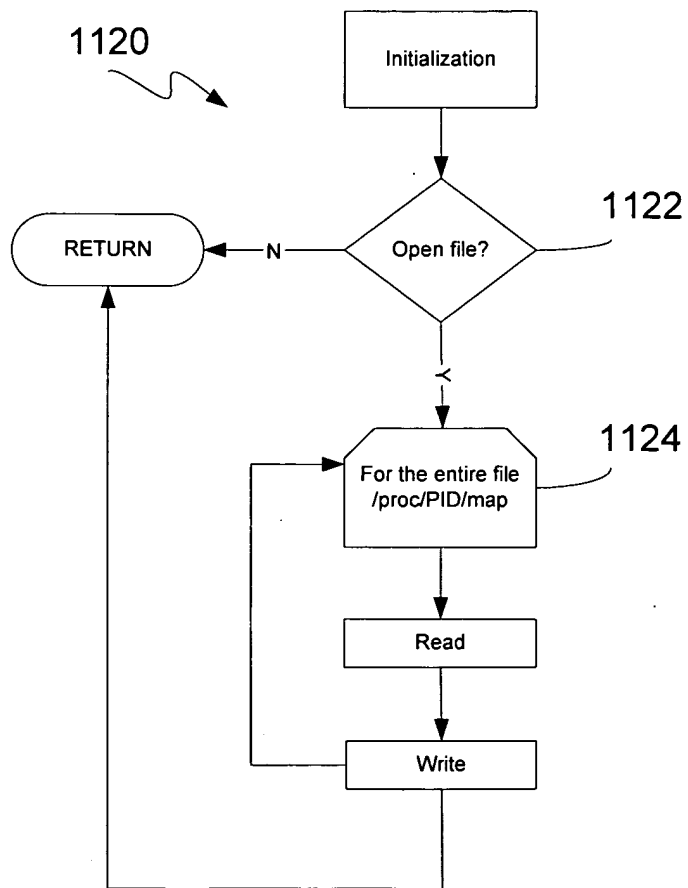


FIG. 11(e)

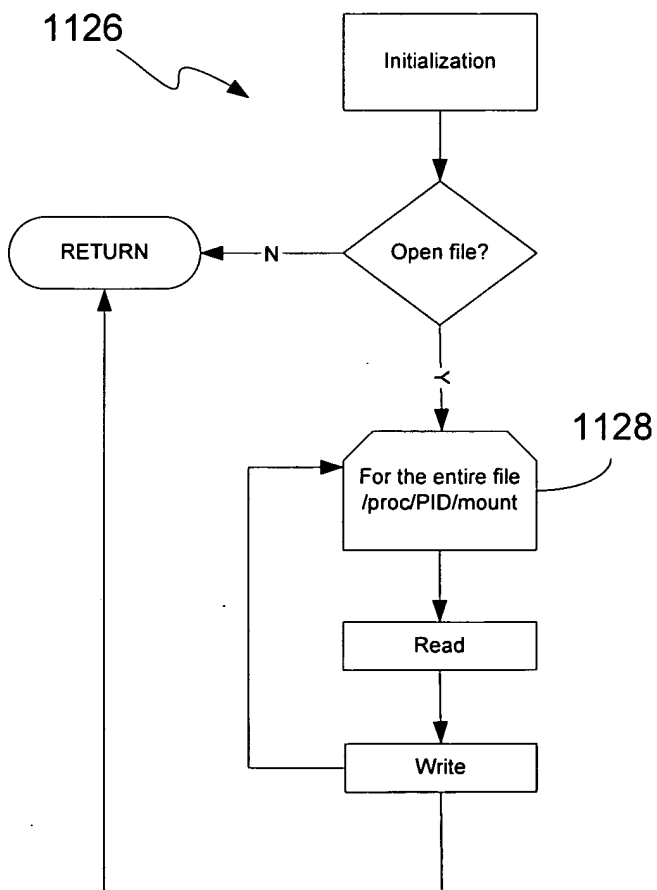


FIG. 11(f)



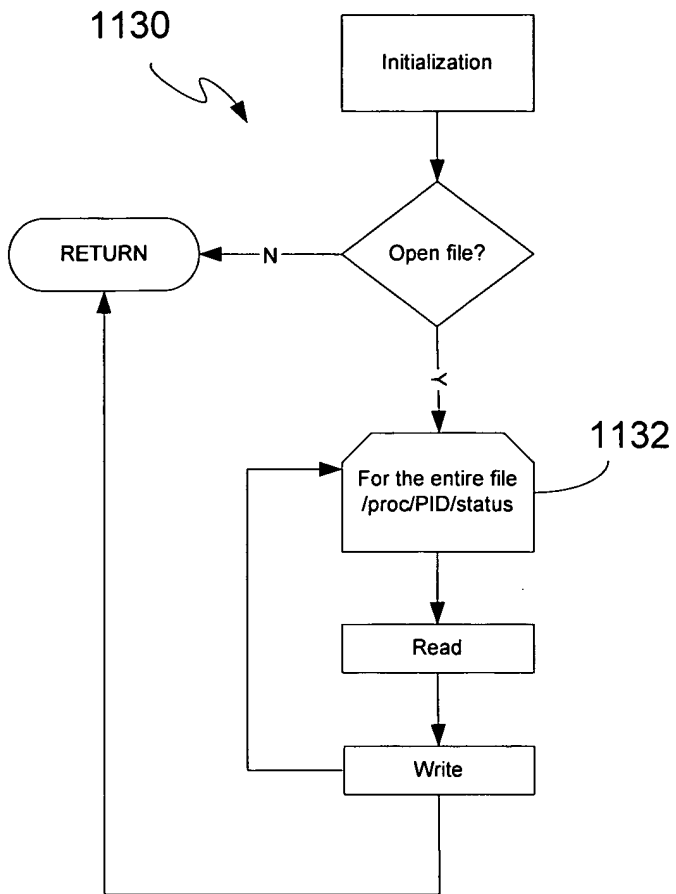


FIG. 11(g)

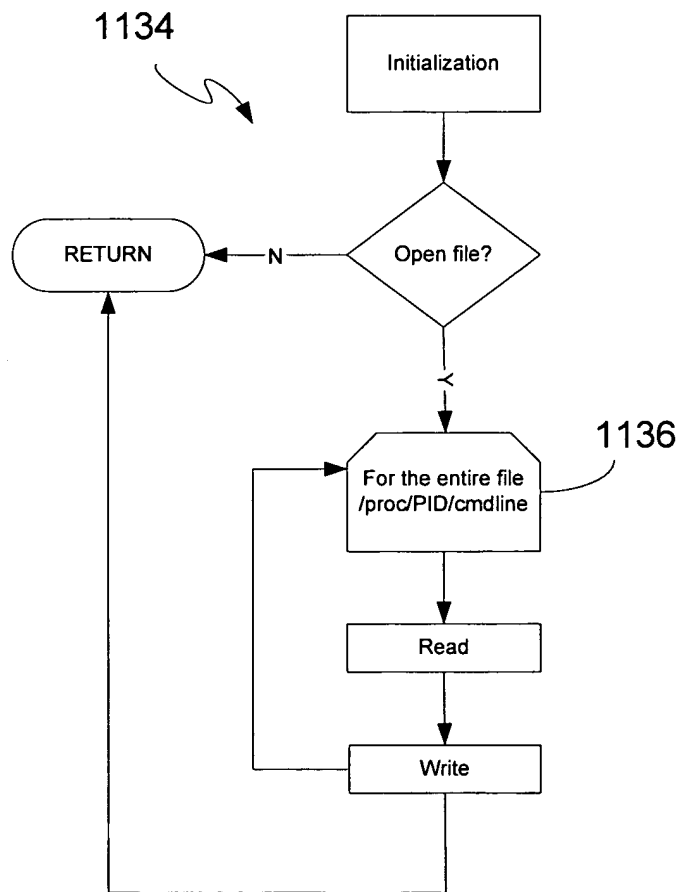


FIG. 11(h)

Running Process Listing - Netscape

### Running Process Listing

Process	Proc Image	Main Image	File Descriptors	Environment	Mapping	Command	Mounts	Status
init	1	1	0	env	map	command	mount	status
vmware-guestd	327	327	4	env	map	command	mount	status
dhclient	329	329	3	env	map	command	mount	status
syslogd	382	382	2	env	map	command	mount	status
klogd	386	386	2	env	map	command	mount	status
portmap	603	603	5	env	map	command	mount	status
rpc.statd	622	622	7	env	map	command	mount	status
apmd	703	703	2	env	map	command	mount	status
sshd	741	741	4	env	map	command	mount	status
xinetd	755	755	6	env	map	command	mount	status
sendmail	778	778	6	env	map	command	mount	status
sendmail	788	788	4	env	map	command	mount	status
gpm	798	798	2	env	map	command	mount	status
crond	807	807	5	env	map	command	mount	status
xfs	841	841	6	env	map	command	mount	status
ard	859	859	4	env	map	command	mount	status
login	862	862	0	env	map	command	mount	status

87  FIG. 11(i)

```
total 13696
drwxr-xr-x  2 root    root      4096 Jan  5 19:41 .
drwxr-xr-x 11 root    root      4096 Jan  5 22:26 ..
-rwxr-xr-x  1 root    root     33960 Jan  5 19:40 1.exe
-rwxr-xr-x  1 root    root     33960 Jan  5 19:40 1.mem_exe
-rwxr-xr-x  1 root    root    103165 Jan  5 19:40 327.exe
-rwxr-xr-x  1 root    root    103165 Jan  5 19:40 327.mem_exe
-rwxr-xr-x  1 root    root    390950 Jan  5 19:40 529.exe
-rwxr-xr-x  1 root    root    390950 Jan  5 19:40 529.mem_exe
-rwxr-xr-x  1 root    root    33635 Jan  5 19:40 582.exe
-rwxr-xr-x  1 root    root    33635 Jan  5 19:40 582.mem_exe
-rwxr-xr-x  1 root    root    28571 Jan  5 19:40 586.exe
-rwxr-xr-x  1 root    root    28571 Jan  5 19:40 586.mem_exe
-rwxr-xr-x  1 root    root    40144 Jan  5 19:40 603.exe
-rwxr-xr-x  1 root    root    38147 Jan  5 19:40 603.mem_exe
```

FIG. 12(a)

```
fd: 0 READ-WRITE /socket:/(1103)
fd: 1 WRITE-ONLY /var/log/messages
fd: 2 WRITE-ONLY /var/log/secure
fd: 3 WRITE-ONLY /var/log/maillog
fd: 4 WRITE-ONLY /var/log/cron
fd: 5 WRITE-ONLY /var/log/spooler
fd: 6 WRITE-ONLY /var/log/boot.log
```

FIG. 12(b)

```

SSH_AGENT_PID=4606
HOSTNAME=sring-1.internal.vlan.iwc.sytexinc.com
PVM_RSH=/usr/bin/rsh
SHELL=/bin/bash
TERM=xterm
HISTSIZE=1000
GTK_RC_FILES=/etc/gtk/gtkrc:/root/.gtkrc-1.2-gnome2
WINDOWID=27270368QTDIR=/usr/lib/qt-3.1
USER=root
LS_COLORS=
PVM_ROOT=/usr/share/pvm3
SSH_AUTH_SOCK=/tmp/ssh-XX3Bs0yB/agent.4542
SESSION_MANAGER=local/sring-1.internal.vlan.iwc.sytexinc.com:/tmp/.ICE-
unix/4542
USERNAME=root
MAIL=/var/spool/mail/root
PATH=/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin
:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin:/root/bin:/usr/local/netscape
INPUTRC=/etc/inputrc
PWD=/root
XMODIFIERS=@im=none
LANG=en_US.UTF-8
LAMHELPPFILE=/etc/lam/lam-helpfile
GDMSESSION=Default
SSH_ASKPASS=/usr/libexec/openssh/gnome-ssh-askpass
HOME=/root
SHLVL=2X
PVM_ROOT=/usr/share/pvm3/xpvm
GNOME_DESKTOP_SESSION_ID=Default
BASH_ENV=/root/.bashrc
LOGNAME=root
LESSOPEN=|/usr/bin/lesspipe.sh %s
DISPLAY=:0.OG_
BROKEN_FILENAMES=1
COLORTERM=gnome-terminal
XAUTHORITY=/root/.Xauthority=/usr/bin/ssh

```

93

FIG. 12(c)

```

rootfs / rootfs rw 0 0
/dev/root / ext3 ro 0 0
/proc /proc proc rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/sdal /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
none /dev/shm tmpfs rw 0 0
none /mnt/hgfs vmware-hgfs rw,nosuid,nodev 0 0
/dev/sdb1 /mnt vfat rw 0 0

```

95

FIG. 12(d)

```

Name:    vmware-guestd
State:   R (running)
Tgid:    327
Pid:     327
PPid:    1
TracerPid: 0
Uid:     0      0      0      0
Gid:     0      0      0      0
FDSize:  32
Groups:
VmSize:  1424 kB
VmLck:    0 kB
VmRSS:    444 kB
VmData:   48 kB
VmStk:     8 kB
VmExe:    84 kB
VmLib:   1252 kB
SigPnd:  0000000000000000
SigBlk:  0000000000000000
SigIgn:  8000000000000000
SigCgt:  00000000000004a07
CapInh:  0000000000000000
CapPrm:  00000000fffffeff
CapEff:  00000000fffffeff

```

97

FIG. 12(e)